Luís Adriano Borges Miranda

Introdução ao Estudo de Curvas Elípticas

Licenciatura em Matemática

ISE/2006

Luís Adriano Borges Miranda

Introdução ao Estudo de Curvas Elípticas

Trabalho Científico apresentado no ISE para a obtenção do grau de Licenciatura em Matemática, sob a orientação da Doutora Natália Furtado.

O júri,

_____

_____

_____

Praia, aos _____ de _____ de _____

AGRADECIMENTOS

Aproveito esta oportunidade para agradecer:

A Deus e à minha mãe por me terem dado vida, força e coragem para enfrentar todos os desafios que têm surgido na minha vida; à Doutora. Natália Furtado que incansavelmente se disponibilizou em me apoiar com sugestões e críticas para uma melhoria na elaboração deste trabalho, colocando à minha disposição documentos de apoio e esclarecendo dúvidas; e, a todos que me apoiaram directa ou indirectamente mas que não foi possível mencionar o nome.

A TODOS UM MUITO OBRIGADO!

Índice

PÁG.

I – INTRODUÇÃO

A construção e o desenvolvimento da Matemática têm constituído uma permanente aventura do homem. O seu passado é premiado por alguns dos mais notáveis e brilhantes pensamentos de várias civilizações.

A ideia deste trabalho cujo tema é "**Introdução ao Estudo de Curvas Elípticas**" surgiu a partir dos problemas da Teoria dos Números, cuja resolução se baseia nas transformações algébricas e interpretação geométrica.

O objecto da pesquisa são curvas elípticas. Existem vários caminhos para chegar a esse conceito. Um dos quais se apresenta neste trabalho. A saber: a partir dos problemas da teoria elementar dos números, cuja resolução pressupõe construção de equações do terceiro grau de duas incógnitas e a sua interpretação geométrica por meio dos respectivos gráficos, chamados curvas cúbicas; introduzindo os conceitos de curvas notáveis, chegamos ao objecto da nossa pesquisa – Curvas Elípticas.

Ciente da relevância e pertinência do tema pretendem-se alcançar os seguintes objectivos:

- Mostrar a interdisciplinaridade entre as diversas áreas da Matemática;
- Estudar analiticamente as curvas elípticas;
- Apresentar ilustrações e algumas demonstrações de propriedades das curvas elípticas;
- Aprofundar conceitos básicos da Álgebra, Geometria Analítica, Teoria dos Números e Geometria Diferencial estudados durante o curso.

Para atingir esses objectivos adoptamos uma metodologia baseada na recolha, análise e tratamento de dados bibliográficos e pesquisas na Internet.

Como se trata de um trabalho de carácter científico, tentamos imprimir o máximo de rigor e originalidade ao longo do seu desenvolvimento. Com base neste princípio, teve-se o cuidado de consultar vários documentos e julgou-se por bem fazer o estudo da seguinte forma: uma pequena abordagem dos problemas da Teoria dos Números até o conceito das curvas elípticas; propriedades das curvas elípticas, torção, rango, e por último o teorema de Mordell-Weil.

II – ESTUDO DE CURVAS ELÍPTICAS

2.1 – Introdução do Conceito de Curva Elíptica

Para chegar ao conceito de curva elíptica pode-se partir da consideração dos problemas da Teoria Elementar dos Números, formuladas da seguinte forma:

A. Encontrar todos os pares dos números naturais m e n tais que a soma dos primeiros m números naturais é igual à soma dos quadrados de primeiros n números naturais.

B. Para que n a soma dos quadrados de primeiros n números naturais é quadrado de um número natural?

C. Quais os números naturais são simultaneamente um produto de dois números naturais sucessivos e um produto de três números naturais sucessivos?

D. Mostrar que a equação $x^3 + y^3 = z^3$ não tem soluções (de números) naturais (Grande Teorema de Fermat para expoente três).

E. Quando é que a soma do quadrado de um número racional e cubo desse mesmo número racional é cubo de um número racional?

F. Quando é que a soma do quadrado de um número racional e cubo desse mesmo número racional é quadrado de um número racional?

Estes problemas podem ser escritos na linguagem algébrica, isto é, representados por meio de equações do 3º grau a duas incógnitas m e n (ou x e y).

Resolver os problemas anteriormente referidos equivale a resolver em números naturais as seguintes equações, respectivamente:

A. $\frac{m(m+1)}{2} = \frac{n(n+1)(2n+1)}{6}$

B. $\frac{n(n+1)(2n+1)}{6} = m^2$

C. $m(m+1) = (n-1)n(n+1)$

D. $x^3 + y^3 = z^3$, pela substituição $x = \frac{x}{z}$ e $y = \frac{y}{z}$ a equação à forma: $x^3 + y^3 = 1$

E. $x^2 + x^3 = y^3$

F. $x^2 + x^3 = y^2$

Geometricamente, cada uma das equações obtidas representa o gráfico da respectiva função. As figuras abaixo ilustram isso de seguinte maneira:

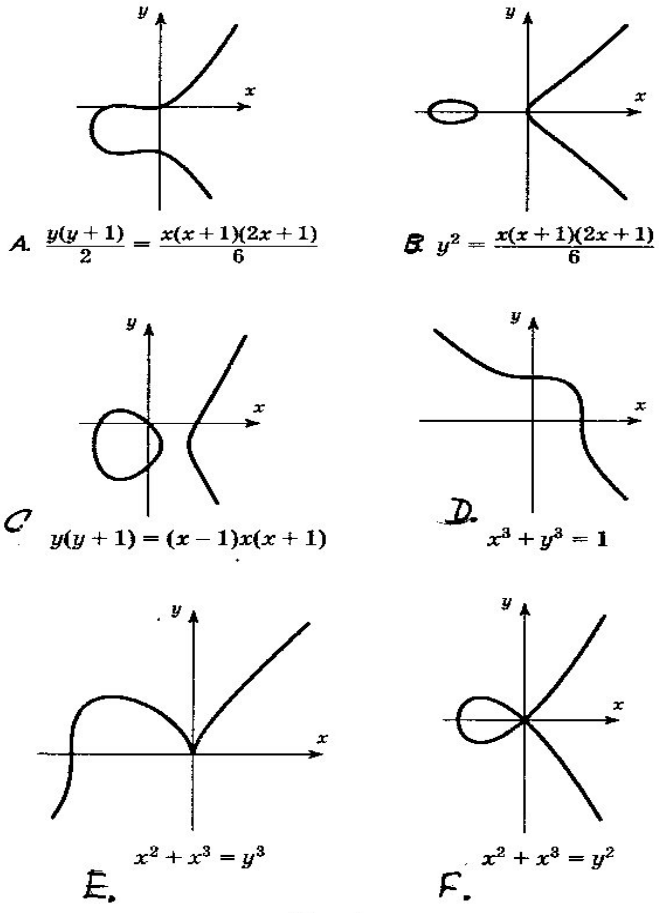

Fig. 1

A questão é, pois, encontrar as coordenadas inteiras ou racionais dos pontos ou, simplesmente, os pontos inteiros ou racionais, que pertencem aos gráficos – curvas cúbicas (ou de terceiro grau). Ou seja, esses problemas reduzem-se ao estudo de soluções inteiras ou racionais das equações cúbicas de duas incógnitas.

Podemos abordar estes problemas mediante técnicas da teoria algébrica de polinómios, isto é, utilizando a factorização real sobre um corpo. Sem dúvida que nalguns casos os trataremos de ponto de vista geométrico.

Pontos racionais e pontos inteiros, na realidade o estudo que vamos fazer centra-se principalmente na procura de pontos com coordenadas racionais, se bem que em muitos casos e da forma mais ou menos indirecta, permitirá ocuparmos das soluções inteiras.

Uma curva elíptica sobre um corpo K é uma curva projectiva regular de género 1 definida por equações com coeficientes em K e que tem pelo menos um ponto racional.

Uma equação de duas incógnitas define uma curva no plano. Sendo que as nossas curvas estão dadas pelas equações do terceiro grau, elas são exemplos das curvas do terceiro grau ou curvas cúbicas.

É visível que as curvas E e F diferenciam-se das outras curvas: a primeira delas tem o **ponto de regresso**, a segunda o **ponto de auto-intersecção**. Esses pontos são exemplos de pontos notáveis de uma curva.

Definição 2.1.1: O ponto (x_0, y_0) da curva $F(x, y) = 0$ chama-se não notável, se por ela passa, pelo menos uma recta $x = x_0 + at$ e $y = y_o + bt$ tal que $t = 0$ é raiz simples da equação $F(x_0 + at, y_0 + bt) = 0$. Caso contrário, o ponto (x_0, y_0) chama-se notável.

As curvas que têm pelo menos um ponto notável, chamam-se curvas notáveis. E as que não têm pontos notáveis, chamam-se não notáveis ou suaves. (São exemplos as curvas dos problemas A – D).

Definição 2.1.2: Seja a curva dada pela equação $f(x,y)=0$; além disso o polinómio $f(x,y)$ não se decompõe em produto de polinómios de grau não superior ao nulo e, também no caso dos polinómios de coeficientes complexos, chama-se a este tipo de curvas, curvas absolutamente irredutíveis.

Se existem os polinómios $F(c)$, $G(c)$ e $H(c)$ com coeficientes racionais, tais que pelo menos uma das funções $\frac{F(c)}{H(c)}$ e $\frac{G(c)}{H(c)}$ não é constante e pela substituição $x=\frac{F(c)}{H(c)}$, $y=\frac{G(c)}{H(c)}$ em $f(x,y)$ obtemos zero (idêntico), então a nossa curva chama-se **racional.** Sendo que a razão de dois polinómios chama-se **função racional**.

Infelizmente, uma curva cúbica não notável nunca é racional. Agora, o que fazer com essas curvas? Em primeiro lugar, o que se pode fazer é reduzi-las ao aspecto mais simples. Para isso utilizaremos as substituições projectivas das coordenadas, isto é, substituições da forma:

$$x'=\frac{\alpha_1 x+\alpha_2 y+\alpha_3}{\gamma_1 x+\gamma_2 y+\gamma_3};\ y'=\frac{\beta_1 x+\beta_2 y+\beta_3}{\gamma_1 x+\gamma_2 y+\gamma_3};$$

Onde, $\gamma_1^2+\gamma_2^2+\gamma_3^2\neq 0$

Tais substituições são muito cómodas, mas elas têm uma deficiência: elas não são definidas em toda a parte (por exemplo, quais são os valores de x' e y' para os pontos da recta $\gamma_1 x+\gamma_2 y+\gamma_3=0$?).

Notemos, que a recta $\gamma_1 x+\gamma_2 y+\gamma_3=0$ intersecta a curva cúbica em não mais do que três pontos; se o nosso objectivo fosse resolução da equação cúbica em números racionais (naturais, inteiros), nós podíamos, primeiramente, considerar todos os pontos de intersecção com essa recta, e depois efectuar substituição projectiva das coordenadas.

Definição 2.1.3: Uma curva cúbica no plano (x, y) chama-se curva na forma de Weierstrass, se ela é dada pela equação:

$$y^2 = x^3 + ax + b$$

Proposição 2.1.1: Curva na forma de Weierstrass é notável se e só se $4a^3 + 27b^2 = 0$.

O número $\Delta = 4a^3 + 27b^2$ chama-se discriminante da cúbica e também, do polinómio $x^3 + ax + b$.

Proposição 2.1.2: O discriminante do polinómio anula-se se e só se o polinómio tem uma raiz múltipla.

Teorema (Newton) 2.1.1: Para qualquer curva cúbica não notável, existem substituições projectivas das coordenadas que a transformam na forma de Weierstrass.

Além disso, se os coeficientes da equação da curva inicial são racionais e a curva tem pelo menos um ponto racional, então podemos encontrar substituições projectivas com $\alpha_i, \beta_i, \gamma_i$ onde $(i = 1,2,3)$ racionais, que transformam a curva inicial em curva na forma de Weierstrass com a e b racionais.

Não vamos demonstrar esse teorema, mas ilustrá-lo-emos nos exemplos dos problemas A – D.

A. Depois da substituição $m = \frac{y-9}{18}$ e $n = \frac{x-3}{6}$ obtemos a equação:

$$y^2 = x^3 - 9x + 81$$

B. Com a substituição $m = \frac{y}{72}$ e $n = \frac{x-6}{12}$ a equação reduz-se à forma:

$$y^2 = x^3 - 36x$$

C. Com a substituição $m = y - \frac{1}{2}$ e $n = x$ a equação reduz-se à forma:

$$y^2 = x^3 - x + \frac{1}{4}$$

D. A curva de Fermat $x^3 + y^3 = 1$ é um caso mais interessante (Ver figura 1)

Agora, observemos com a ajuda de algumas figuras, como se processam tais substituições projectivas das coordenadas (Ver figuras 2 e 3 respectivamente):

a) Dada a curva $x^3 + y^3 = 1$;

b) Substituição $x = s - t$, $y = t$ - projecção paralela do plano xOy sobre o plano sOt;

c) Curva $s^3 - 3s^2t + 3st^2 = 1$;

d) Substituições $s = \frac{1}{3u}$, $t = \frac{6v+1}{6u}$ - projecção central do plano sOt sobre o plano uOv;

e) Curva $v^2 = u^3 - \frac{1}{108}$ (na forma de Weierstrass).

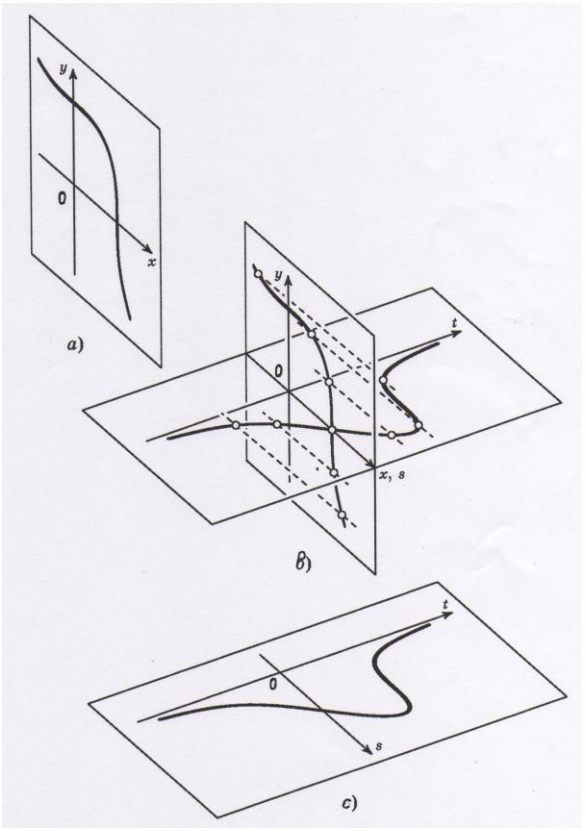

fig. 2

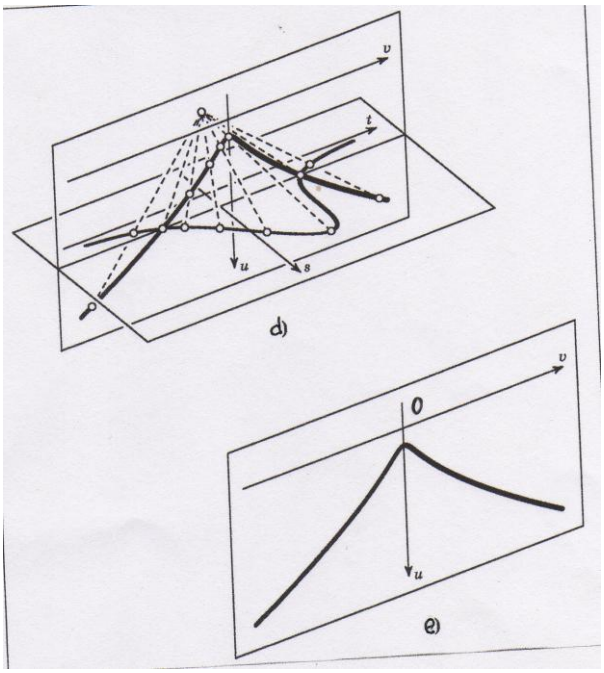

fig. 3

Definição 2.1.4: Uma curva não notável do terceiro grau chama-se **Curva Elíptica**.

O Teorema de Newton afirma que toda a curva elíptica obtida por meio de uma substituição projectiva das coordenadas se reduz à forma de Weierstrass.

Se o discriminante $\Delta = 4a^3 + 27b^2$ da curva $y^2 = x^3 + ax + b$ é nulo, então essa curva é racional.

No futuro, vamos entender uma curva elíptica como uma curva não notável do terceiro grau, dada por uma equação com coeficientes racionais. (Normalmente tais curvas chamam-se curvas elípticas sobre corpo de números racionais.).

Se sobre tal curva se encontra, pelo menos, um ponto racional, então essa curva pode ser reduzida à forma de Weierstrass pela substituição projectiva das coordenadas com α_i, β_i, γ_i $(i = 1,2,3)$ racionais.

2.2 - Adição dos Pontos de uma Curva Elíptica e Suas Propriedades

Os problemas A – C são equivalentes à procura de todos os pontos de coordenadas inteiras em curvas elípticas; no problema D exige-se encontrar todos os pontos com coordenadas racionais numa curva elíptica.

O método de Sócrates permite introduzir no conjunto de pontos racionais duma curva elíptica uma estrutura. A saber, os pontos racionais numa curva elíptica podem ser "multiplicados".

Suponhamos, que nós encontramos na curva elíptica $y^2 = x^3 + ax + b$ dois pontos racionais $P(x_P, y_P)$ e $Q(x_Q, y_Q)$. (Ver figura 4)

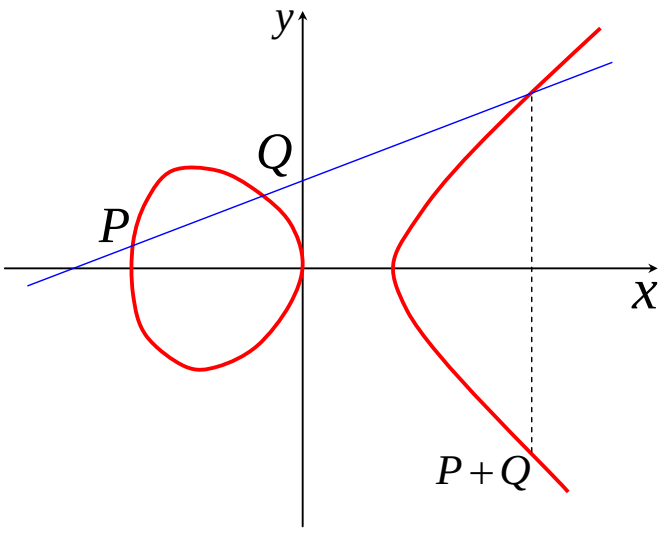

fig. 4

Tracemos a recta PQ e calculemos as coordenadas do terceiro ponto da intersecção da recta com a curva. Essas coordenadas satisfazem ao sistema de equações:

$$\begin{cases} y^2 = x^3 + ax + b \\ (y - y_P)(x_Q - x_P) = (x - x_P)(y_Q - y_P) \end{cases}$$

Se $x_P \neq x_Q$ e $y_P \neq y_Q$, então, exprimindo da segunda equação x através de y, substituímos x da primeira equação pela expressão obtida. Em resultado, chegamos à equação cúbica de y com coeficientes racionais. Sendo que duas raízes dessa equação são racionais (elas são y_P e y_Q), a soma de todas as três raízes é um número racional. (Pelo teorema de Viéte).

Isso significa então que a terceira raiz também é racional. Assim, por dois pontos racionais, situados numa curva elíptica, nós construímos o terceiro ponto racional. Mais um ponto racional obtém-se da construção do ponto simétrico em relação ao eixo Ox. Esse ponto simétrico chama-se soma dos pontos P e Q e designa-se $P+Q$ (fig. 4)

Vejamos agora uma questão: como calcular o ponto $P+P=2P$

Quando os pontos foram diferentes, nós traçamos por eles uma recta. Sendo que eles coincidem, é claro que é preciso uma tangente (fig. 5)

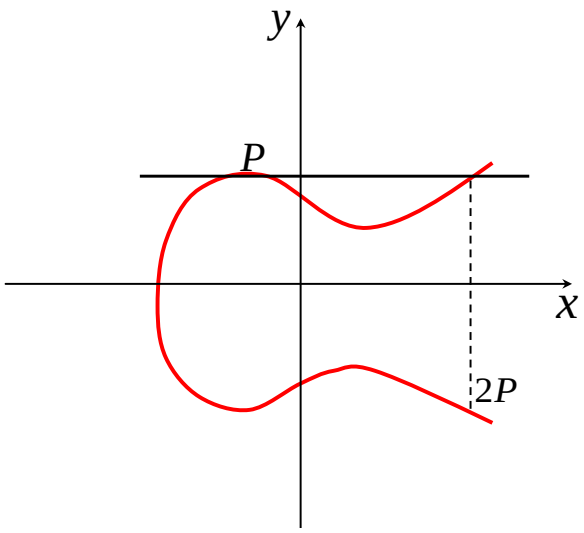

fig.5

O que fazer para encontrar $3P$? É simples, consideramos a soma $2P$ e P.

Analogamente, pode-se calcular $4P = 3P + P$, $5P = 4P + P$ etc.

É notável que a adição dos pontos de uma curva elíptica que nós introduzimos goza de algumas propriedades dos números reais:

a) Comutatividade (para quaisquer pontos P e Q duma curva elíptica tem que verificar a identidade $P+Q=Q+P$);

b) Existência de um elemento nulo (tal ponto O, que $P+O=P=O+P$ para qualquer ponto P);

c) Existência do ponto oposto para qualquer ponto P de uma curva elíptica (tal ponto $-P$, tal que $P+(-P)=O=-P+P$);

d) Associatividade (para quaisquer pontos P, Q e R de uma curva elíptica tem que se efectuar a identidade $(P+Q)+R=P+(Q+R)$).

Verifiquemos essas propriedades

- Comutatividade – Para o cálculo do ponto $Q+P$ utilizaremos a mesma recta, que utilizámos para o cálculo do ponto $P+Q$, consequentemente, $P+Q=Q+P$.

- Existência do nulo e do ponto oposto

Seja P um ponto sobre a curva dada com mostra a figura:

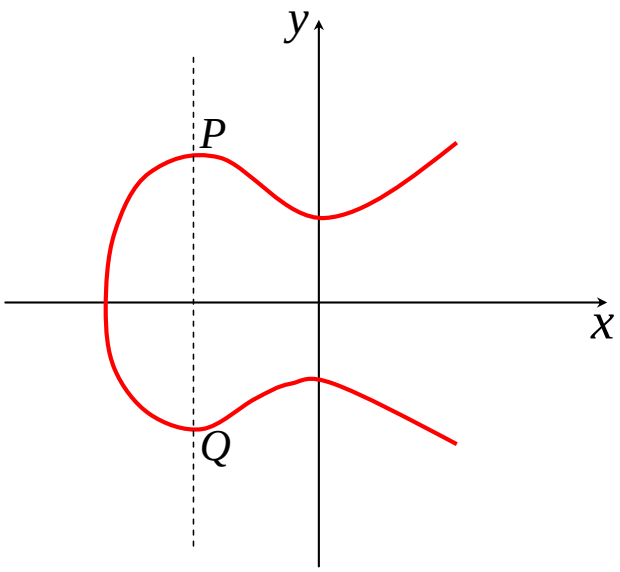

fig. 6

Nós pretendemos encontrar um ponto tal que, se traçarmos uma recta por ela e o ponto P, intersecta essa recta com a curva e depois reflectir o ponto de intersecção em relação ao eixo Ox, então novamente se obtém o ponto P.

Designemos por Q o ponto simétrico de P relativamente ao eixo Ox. De tudo o que foi dito, segue-se que a recta deve passar por P e Q, isto é, deve ser vertical. Consequentemente, o ponto O deve estar tal sobre a curva, como sobre qualquer recta vertical que intersecta a curva.

Tal ponto não está no plano. Mas nós precisamos muito dele. Por isso adicionamo-lo ao plano e chamar-lhe-emos Ponto Infinitamente Afastado, designando-o pelo símbolo "∞". Vamos concluir que ∞ é o ponto de intersecção de todas as rectas verticais.

Contudo, dessa forma o ponto $O=\infty$ nós adicionarmos formalmente. Sabemos que a recta que passa por ∞ e por qualquer ponto Q é uma recta vertical. Por essa razão é correcto considerar o ponto O como ponto racional.

A recta vertical que passa por P também passa por $O=\infty$. Por isso, Q que é um ponto de intersecção dessa recta com a curva elíptica, satisfaz a relação $P+Q=0$, isto é, é oposta a P. Isso significa que, qualquer ponto P tem oposto $Q=-P$, simétrico relativamente ao eixo Ox. Notemos que para os pontos P situados no eixo das abcissas, se tem $-P=P$.

- Associatividade

Marquemos na curva elíptica dada os pontos P, Q e R como mostra a figura 7.

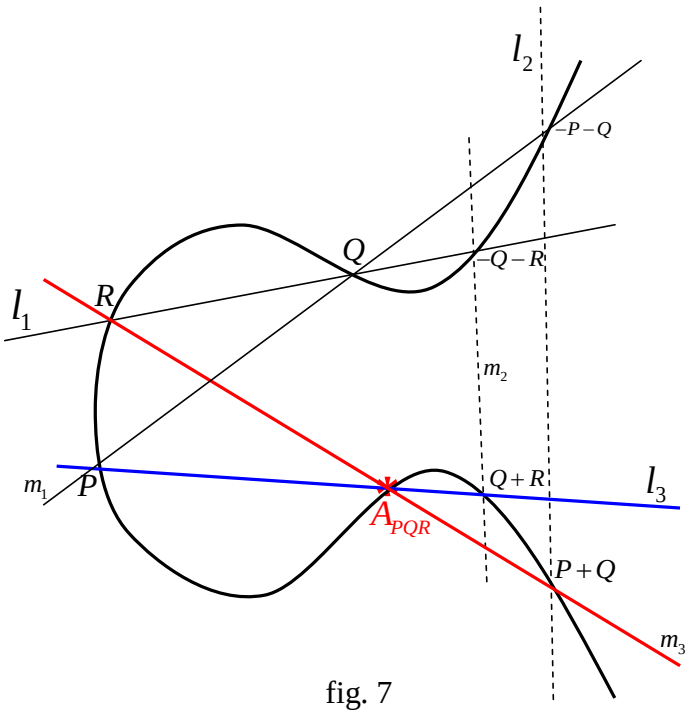

fig. 7

Construiremos os pontos $-P-Q$ e $-Q-R$, que são pontos de intersecção das rectas $\overline{PQ}$ e $\overline{RQ}$ com a curva, respectivamente, e também os pontos $P+Q$ e $Q+R$.

Para mostrar a igualdade $(P+Q)+R=P+(Q+R)$, basta mostrar que o ponto de intersecção da recta, que passa por $P+Q$ e R, com a recta, que passa por P e $Q+R$ pertence à curva.

A configuração de seis rectas $l_1, l_2, l_3, m_1, m_2, m_3$ (que passam pelos pontos Q e R; $-P-Q$ e $P+Q$; P e $Q+R$; P e Q; $-R-Q$ e $Q+R$; R e $P+Q$ respectivamente), esquematicamente representado na figura:

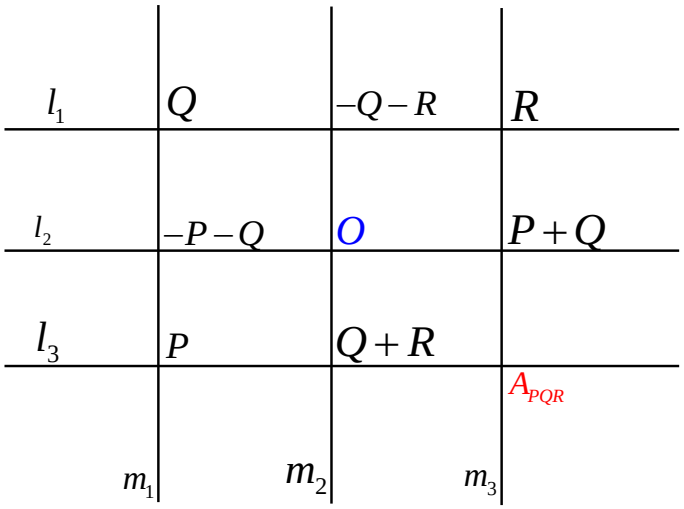

fig. 8

Cada uma das rectas mencionadas passa por três pontos (as rectas, que passam por $-R-Q$ e $Q+R$; $-P-Q$ e $P+Q$ passam por $O=\infty$), num total de nove pontos que pertencem à curva elíptica, **E** da equação $F(x,y)=0$.

O nosso objectivo é mostrar que o nono ponto A_{PQR} pertence a nossa curva E.

Sejam:

$L_1(x,y)=0$; $L_2(x,y)=0$; $L_3(x,y)=0$

$M_1(x,y)=0$; $M_2(x,y)=0$; $M_3(x,y)=0$ as equações das rectas $l_1, l_2, l_3, m_1, m_2, m_3$, respectivamente.

Mostremos que:

$F(x,y)=\alpha L_1(x,y)L_2(x,y)L_3(x,y)+\beta M_1(x,y)M_2(x,y)M_3(x,y)$, onde α e β são números quaisquer.

Consideremos a diferença:

$$F-(\alpha L_1L_2L_3+\beta M_1M_2M_3) \qquad (1)$$

Essa diferença é um polinómio de x e y de grau não superior a três. Esse polinómio é igual ao nulo nos pontos P, $-P-Q$ e Q.

Escolhemos na recta m_1 mais um ponto $S=(s_1,s_2)$, distinto de P, $-P-Q$ e Q. O ponto S não está situado sobre nenhuma das rectas l_1, l_2, l_3 e consequentemente, $L_1(s_1,s_2)\neq 0$, $L_2(s_1,s_2)\neq 0$, $L_3(s_1,s_2)\neq 0$ mas $M_1(s_1,s_2)=0$.

Substituímos as coordenadas dos pontos S na diferença **(1)** e encontramos α da equação:

$F(s_1,s_2)-\alpha L_1(s_1,s_2)L_2(s_1,s_2)L_3(s_1,s_2)=0$,com tal escolha de α a diferença (1) anula-se nos quatros pontos P, $-P-Q$, Q e S da recta m_1.

Nós escolhemos o parâmetro α tal que, a diferença (1) se divide por M_1. Considerando os pontos Q, $-R-Q$ e R na recta l_1, analogamente encontramos o parâmetro β tal que, a diferença (1) se divide L_1. Verificamos que a diferença (1) se representa na forma $L_1(x,y)M_1(x,y)N(x,y)$, onde $N(x,y)$ é um polinómio de grau não superior a 1 (um). Se esse polinómio é igual a 1 (unidade), então a equação $N(x,y)=0$ representa uma recta n.

Assim, $F-(\alpha L_1L_2L_3+\beta M_1M_2M_3)=L_1M_1N$. Substituímos nessa igualdade as coordenadas do ponto $P+Q$. Na parte esquerda obtêm-se o polinómio nulo. Se nem L_1, nem M_1 não se anulam, então $N=0$, o que significa que o ponto $P+Q$ pertence à recta n (ou que $P+Q$ está sobre a recta n). Analogamente concluímos que o ponto $Q+R$ pertence à recta n. Se fosse infinito um ponto habitual, então obteríamos, da mesma maneira, que ela pertenceria à recta n.

É óbvio que, no caso geral, pelo facto de as rectas l_1 e m_1 não serem verticais, não segue, que a recta que passa pelos pontos $P+Q$ e $Q+R$, é vertical. Por isso o polinómio N tem grau nulo, isto é, é uma constante. Mas o polinómio N anula-se no ponto $P+Q$, e consequentemente, ele é idêntico ao nulo.

Desse modo, $F(x,y)=\alpha L_1(x,y)L_2(x,y)L_3(x,y)+\beta M_1(x,y)M_2(x,y)M_3(x,y)$, e o ponto A_{PQR}, cujas coordenadas se determinam do sistema de equações

$$\begin{cases} L_3(x,y)=0 \\ M_3(x,y)=0 \end{cases}$$ está situado na curva $F(x,y)=0$.

Com isso, nós mostramos a associatividade da adição dos pontos com algumas pressuposições complementares:

- Nenhum dos pontos da fig. 8 coincidem;
- As rectas l_1 e m_1 não passam pelo ponto $P+Q$;
- As rectas que passam pelos pontos $P+Q$, $Q+R$ e também as rectas l_1 e m_1 são perpendiculares.

2.3 – Abordagem algébrica do conceito. Propriedades. Teoremas.

Introduzindo o conceito de plano projectivo, o objecto da nossa consideração pode ser representado da seguinte maneira:

Definição 2.3.1: Um conjunto S é um plano projectivo se existem subconjuntos $l_1, l_2, ...$ de S que satisfazem as seguintes propriedades:

(i) Se P e Q pertencem a S, um e somente um dos subconjuntos l_i contém P e Q;

(ii) A intersecção de l_i e l_j consiste sempre num único elemento, para todo $i \neq j$;

(iii) Existem pelo menos quatro elementos de S tais que, entre eles não haja três contidos em um dos subconjuntos l_i.

Nota: Os elementos de S são normalmente chamados pontos e os subconjuntos l_i rectas.

Definição 2.3.2: Uma curva elíptica sobre um corpo K é uma cúbica regular de um plano projectivo IP_2 (K).

Apesar de não ser imprescindível, suponhamos sempre que a curva em questão possui um ponto racional, que chamaremos de O. Então toda a curva elíptica é, portanto, o lugar projectivo de um polinómio da forma:

$$p\left(x_1, x_2, x_3\right) = \sum_{i+j+k=3} a_{ijk} x_1^i x_2^j x_3^k \quad , a_{ijk} \in K \tag{1}$$

A forma (1) pode ser simplificada numa forma muito mais simples e fácil de trabalhar e para isso, vamos construir o nosso raciocínio com base na seguinte propriedade:

Propriedade 2.3.1. Toda a curva elíptica é isomorfa a uma curva definida por um polinómio da forma:

$$x_2^2 x_3 + a_1 x_1 x_2 x_3 + a_3 x_2 x_3^2 = x_1^3 + a_2 x_1^2 x_3 + a_4 x_1 x_3^2 + a_6 x_3^3 \tag{2}$$

A forma (2) chama-se forma larga de Weierstrass e é habitualmente utilizada para definir uma curva elíptica. A mesma pode, ainda, ser reduzida numa forma mais simples.

Se passamos para porção afim e fazendo $x_3 = 1$, vamos obter a seguinte forma:

$$y^2 + a_1 xy + a_3 y = x^3 a_2 x^2 + a_4 x + a_6 \tag{3}$$

onde unicamente temos perdido o ponto no infinito $(0{:}1{:}0)$ que chamaremos O.

Uma vez encontrada a forma larga de Weierstrass definem-se as seguintes constantes, que dependem da curva:

$$b_2 = a_1^2 + 4a_2;$$

$$b_4 = 2a_4 + a_1 a_3;$$

$$b_6 = a_3^2 + 4a_6;$$

$$b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2;$$

$$c_4 = b_2^2 - 24b_4;$$

$$c_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6;$$

$$\Delta = -b_2^2 b_8 - 8b_4^3 + 96 b_2 b_4 b_6;$$

$$j = c_4^3 / \Delta.$$

Observe-se como, se ortogonamos a cada a_i o peso i, as constantes anteriores são homogéneas. Daí a substituição, aparentemente tão caprichosa

Seja E uma curva elíptica.

Algumas propriedades interessantes destas constantes são:

a) A curva é não singular se e só se $\Delta \neq 0$;

b) Duas curvas E e E' são isomorfas se e só se $j(E) = j(E')$;

c) Se $P \in E$ é um ponto singular, que tipo de singularidade se pode estabelecer com c_4.

Ainda podemos simplificar mais a equação (3) da curva. Pelo que, agora temos que ter um certo cuidado. Devemos fazer uma mudança de variável que deixa fixo o ponto O do infinito (para manter esse ponto racional) e, se possível, permitir que os coeficientes de y^2 e x^3 sejam unitários. É fácil ver que tal mudança de variável segue as seguintes características:

$$x' = u^2 x + r$$

$$y' = u^3 y + u^2 s x + t$$

Com estas restrições já pelo outro caminho, podemos chegar a curva na forma:

$$y^2 = x^3 + ax + b \qquad (4)$$

Com $a = -27c_4$ e $b = -56c_6$.

Esta forma denomina-se forma breve (curta) de Weierstrass e, como é evidente, suponhamos sempre que o corpo em que estamos a trabalhar tem característica distinta de 2 e 3.

A forma breve de Weierstrass permite-nos estudar como se vêem as curvas elípticas no plano afim real ou racional. Existem duas classes de curvas do ponto de vista gráfico:

1) Aquelas em que $x^3 + ax + b = 0$ tem três raízes reais (fig. 9);
2) Aquelas em que, a mesma equação tem somente uma raiz real (fig. 10).

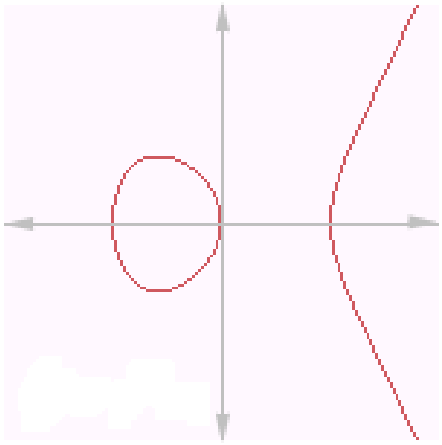

fig. 9

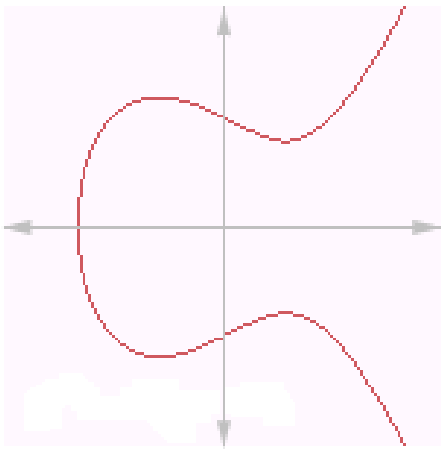

fig. 10

Em ambos os casos, a curva é simétrica em relação ao eixo Ox.

A proposição seguinte é um resultado elementar de curvas algébricas e pode ser encontrado em qualquer livro desta matéria.

Proposição 2.3.2. Toda a recta que corta uma curva elíptica E em dois pontos (contando sua multiplicidade), corta-a em três.

Efeitos práticos, o contar a multiplicidade dos pontos não quer dizer que uma recta tangente a E num ponto P, corta a recta duas vezes em P.

Definição 2.3.3: Numa curva elíptica define-se a seguinte operação interna:

$$+ : E \times E \to E$$

$(P,Q) \mapsto R$, onde o ponto R é simétrico em relação ao eixo Ox e é o terceiro ponto de intersecção da recta PQ com E.

No entanto, pode parecer estranho mas a definição tem sua razão de ser. Em primeiro lugar, não se define $P+Q$ como terceiro ponto de intersecção porque esse facto tornaria impossível definir um elemento neutro para a soma (pode-se fazer, mas não é aconselhável). Ainda definida desta maneira, a operação tem de forma imediata um elemento neutro: o ponto do infinito, que vê assim reforçada sua condição de "ponto especial".

Assim falaremos de outra maneira a introdução da adição já abordada anteriormente.
Este procedimento do cálculo do ponto soma é conhecida por algoritmo de corda tangente (os dois casos possíveis que aparecem) e pode dar-se em termos de coordenadas, facto que vamos ver mais adiante.

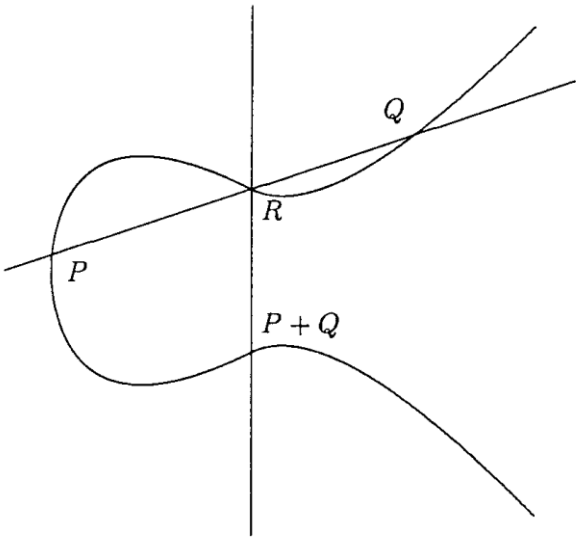

fig. 11

(Algoritmo da corda tangente)

Agora vamos ver que propriedade tem esta operação interna. Na realidade, não possui todas.

Teorema 2.3.1: O par $(E,+)$ é um grupo abeliano.

Algumas propriedades deste grupo abeliano já foram demonstradas anteriormente, pelo que só vamos fazer um pequeno comentário acerca da **transitividade** que é algo mais complexo de demonstrar e requer o teorema de Bezout de intersecção de curvas (ou, pelo menos, alguns dos seus corolários). Outra forma de fazê-lo (menos geométrico) é utilizando a teoria de divisores.

Uma pergunta que surge de maneira imediata é: que aplicações mantém tanto a estrutura geométrica de E como a algébrica? A resposta neste caso é rápida: as mesmas.

Definição 2.3.4: Um morfismo não constante entre duas curvas elípticas denomina-se isogenia.

É possível demonstrar que o facto de não ser constante implica ser, na realidade, um isomorfismo.

Pelo que estas aplicações ainda verificam outro facto importante.

Proposição 2.3.3: Uma isogenia entre duas curvas elípticas é um honomorfismo de grupos.

Assim, todas as nossas manipulações até à forma breve de Weierstrass não mudaram a estrutura de grupo da curva original, ser morfismo e bijectivos e, por tanto, isomorfismo de grupos.

OBS: Neste primeiro contacto com as curvas elípticas, vamos dar uma breve ideia de como introduzir o mesmo conceito de ponto de vista de Análise Complexa.

Da mesma forma que calculamos a forma breve de Weierstrass, pode-se reduzir toda curva a uma da forma:

$$E: y^2 = 4x^3 - \frac{c_4}{12}x - \frac{c_6}{216}$$

Esta equação está claramente relacionada com a conhecida equação diferencial

$(y')^2 = 4y^3 - g_2 y - g_3$, que tem por solução a função de $\wp$ de Weierstrass, função dupla periódica de período, digamos ω_1 e ω_2.

Considerando $\mathbb{C}$, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, é evidente que $\wp$ está bem definida no grupo quociente $\mathbb{C}/\Lambda$ e podemos definir uma aplicação:

$$\phi: \mathbb{C}/\Lambda \to E$$
$$z \notin \Lambda \mapsto \left(\wp(z), \wp'(z)\right)$$
$$z \in \Lambda \mapsto O$$

Debaixo destas condições vamos ter o seguinte.

Teorema 2.3.2: A aplicação anterior é um isomorfismo de grupos e seu inverso é:

$$\phi^{-1}(x, y) = \int_{-\infty}^{x+\frac{b}{12}} \frac{dt}{\sqrt{4t^3 - g_2 t - g_3}}$$

2.4 - Torção

Seja P um ponto sobre uma curva elíptica. Com ele pode-se construir novos pontos $...,-3P,-2P,-P,P,2P,3P,...$. Se o ponto P é racional, então todos esses pontos também são racionais.

São possíveis dois "modelos de comportamento" do ponto P: ou todos os pontos obtidos são distintos, ou entre eles há coincidentes.

No último caso, seja, por exemplo, $mP=nP$, $m>n$. Conforme as regras de adição imediatamente obtemos, que $(m-n)P=0$, isto é, existe um natural k_1 tal que $k_1P=0$.

Definição 2.4.1: Seja k um tal número minimal. O número k chama-se ordem do ponto P e P chama-se ponto de Torção ou ponto de ordem finita.

Notemos que, conforme a definição do ponto O, este é um ponto de torção da ordem 1. No caso do primeiro "modelo de comportamento" diz-se que a ordem do ponto P é igual ao infinito.

É notável que, qualquer curva elíptica contém sempre somente um número finito de pontos de torção. (a demonstração desse facto não é fácil!). Além disso, como mostrou Barri Mazur, para número $\pm$ de pontos racionais da ordem finita sobre uma curva elíptica têm-se somente as seguintes possibilidades:

a) $1\le t\le 10$

b) $t=12$

c) $t=16$

No que se segue, notaremos por $E(\square)[n]$ o conjunto dos pontos de ordem n de $E(\square)$, isto é, aqueles que verificam que $nP=O$.

O subgrupo de torção de $E(\square)$ tem vindo a ser muito estudado e os teoremas que lhe concerne aportam toda a informação que podemos chegar a necessitar acerca deste grupo. O caso de torção de $E(K)$, com K um corpo de números algébricos, é muito menos estudado.

O teorema fundamental em que a torção se refere deve-se a Barry Mazur e a sua demonstração é tão complexa que a única referência onde se pode encontrar completa é no

próprio autor, em Rational points ou modular curves, no volume Modular functions of one variable (Springer LNM).

Teorema 2.4.1: O grupo de torção de $E(\mathbb{Q})$ pertence a um destes quinze tipos:

$$\mathbb{Z}/n\mathbb{Z} \quad n = 1, 2, ..., 10, 12$$

$$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2n\mathbb{Z}) \quad n = 2, 4, 6, 8$$

Já sabemos, portanto, que dado um ponto, a ordem que pode ter o grupo $E(\mathbb{Q})$ não pode ser qualquer, se não um número finito (contando eventualmente com que pode ter ordem infinito). Assim, se podemos reduzir a procura dos pontos de torção a um conjunto finito, teremos claramente um algoritmo "de inspecção" para calcular a torção.

Teorema 2.4.2: (Nagell-Lutz) Seja P um ponto de torção de $E(\mathbb{Q})$, com E uma curva elíptica na forma breve de Weierstrass. Então:

1) As coordenadas de P estão em $\mathbb{Z}$;
2) Ou $P \in E(\mathbb{Q})[2]$, ou as coordenadas de P ao quadrado se dividem $\Delta = 4a^3 + 27b^2$.

Sem dúvida que existe um procedimento muito útil para reduzir a procura ou, em certos casos, para calcula-la directamente: a redução.

Definição 2.4.2: A aplicação redução módulo p define-se como

$$red_p : E(\mathbb{Q}) \to E(\mathrm{F}_p)$$

$P \mapsto red_p(P)$, onde F_p é o corpo com p elementos e $red_p(P)$ é o resultado da redução módulo p a cada coordenada de P. Para que a aplicação esteja bem definida podemos supor que $P = (x : y : z)$, onde x, y, z são inteiros primos entre si.

Por insignificante que possa parecer, esta aplicação contém muita informação sobre a $Tor(E(\mathbb{Q}))$.

Teorema 2.4.3: Com as condições anteriores, red_P é um homomorfismo de grupos, injectiva na sua restrição a $Tor\left(E(\square)\right)$, supondo que p não divide Δ e que não há pontos de ordem p em $E(\square)$.

Deste teorema surge a seguinte definição e o seguinte corolário, baseando também no teorema de Mazur.

Definição 2.4.3: Uma curva E diz-se que tem boa redução em p quando p não divide Δ.

Corolário 2.4.1: A aplicação red_P é injectiva na torção, para todo o primo $p>11$ no que E tenha boa redução. Portanto, um procedimento para calcular a torção poderia ser o seguinte:

Algoritmo de Torção

Dados a e b, coeficientes da forma breve de Weierstrass:

1. Calcular $E(\square)[2]$, resolvendo $x^3+ax+b=0$;
2. Calcular, um conjunto de possíveis pontos de torção;
3. Calcular os múltiplos de cada ponto dos anteriores digamos P, utilizando o algoritmo da corda tangente, até encontrar $12P$, um elemento de $E(\square)[2]$, ou o próprio O;
4. Se $nP\neq O$ para $n=1,2,...,12$, $P\notin Tor\left(E(\square)\right)$. Sem dúvida que, pode ser útil, para reduzir o números de iterações, calcular, para certo número de primos, o cardinal de $E(\mathrm{F}_P)$, seja n_P, tendo em conta que $P>11$ e que não deve dividir Δ.

Como $Tor\left(E(\square)\right)\subset E(\mathrm{F}_P)$, para todos esses p, a ordem de torção deve dividir o máximo divisor comum dos n_P. Na prática um número nesse caso de reduções (cinco ou seis) ajuda a reduzir enormemente a procura, se a torção da curva o permite, obviamente.

2.5 - Rango

O cálculo do rango é mais complexo. Não se conhece nenhum algoritmo que funcione sempre, no entanto se há algoritmos que funcionam em todos os casos conhecidos nos que serão utilizados. O livro de referência é de novo Cremona, J. ; Algorithms for elliptic cuves (Cambrige University Press).

O resultado fundamental desta secção é uma versão algo mais operativa do teorema débil de Mordell-weil na sua versão de 2-descenso.

Definição 2.5.1: Seja E uma curva elíptica, chama-se rango da curva ao número mínimo possível, do teorema de Mordell.

Proposição 2.5.1: Seja E uma curva elíptica na forma $y^2=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, $\alpha_i \in \mathbb{Q}$.

Seja S o conjunto dos primos que dividem Δ união com 2, eventualmente e definimos $\mathbb{Q}(S,2)=\left\{b\in \mathbb{Q}^*/\mathbb{Q}^{*2} : ord_P(b)=0, \forall_P \notin S\right\}$, ou seja, os inteiros múltiplos de elementos de S e não de outros primos e livre de quadrados.

Nestas circunstâncias, existe um homomorfismo de grupos injectivo

$$E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}(S,2)\times \mathbb{Q}(S,2), \text{ definido por}$$

$$P=(x,y)\mapsto \begin{cases} (x-\alpha_1, x-\alpha_2) & se\ x\neq \alpha_1,\alpha_2 \\ \left(\dfrac{\alpha_1-\alpha_3}{\alpha_1-\alpha_2}, \alpha_1-\alpha_2\right) & se\ x=\alpha_1 \\ \left(\alpha_2-\alpha_1, \dfrac{\alpha_2-\alpha_3}{\alpha_2-\alpha_1}\right) & se\ x=\alpha_2 \\ (1,1) & se\ P=0 \end{cases}$$

Seja agora (b_1,b_2) um elemento de $\mathbb{Q}(S,2)^2$, que não seja a imagem de O, $(\alpha_1,0)$ ou de $(\alpha_2,0)$. Então (b_1,b_2) é a imagem de um ponto $P\in E(\mathbb{Q})/2E(\mathbb{Q})$ se e só se o sistema

$$\begin{cases} b_1z_1^2-b_2z_2^2=\alpha_2-\alpha_1 \\ b_1z_1^2-b_1b_2z_3^2=\alpha_3-\alpha_1 \end{cases}, \quad \text{tem solução em } \mathbb{Q}^*\times\mathbb{Q}^*\times\mathbb{Q}, \text{ digamos}$$

(z_1,z_2,z_3).

O ponto P tem como coordenadas $P=\left(b_1z_1^2+\alpha_1, b_1b_2z_1z_2z_3\right)$.

Corolário 2.5.1: Nas condições anteriores

$$\#\left[E(\square)/2E(\square)\right]=2^{2+r}$$

Esta proposição oferece-nos um método "quase-algoritmo" para calcular o rango.

Quase-algoritmo do rango

Dados a e b, coeficientes na forma de Weierstrass:

1. Comprovar que temos três raízes racionais para $x^3+ax+b=0$ ou, o que é igual, que haja três pontos e ordem 2 (no qual se pode fazer com o algoritmo de torção).
2. Calcular o conjunto $\square\left(S,2\right)$.
3. Para cada par de $\square\left(S,2\right)^2$,calcular um ponto do que proceda o grupo $E(\square)/2E(\square)$, vem demonstrar que o sistema associado ao par não tem solução.
4. Calcular o rango seguindo o corolário.

Proposição 2.5.2: Seja E uma curva elíptica na forma breve de Weierstrass $y^2=x^3+ax+b$. Então verifica-se que:

1. Para cada ponto da forma $P=\left(\frac{a}{d^2},\frac{b}{d^3}\right)\in E$, existe uma constante C_P tal que, para todo $Q\in E$, $h\left(P+Q\right)\le 2h\left(P\right)+C_P$, onde se pode tomar $C_P=\ln\left(\left|ad^2\right|+\left|a^2\right|+\left|Ad^2a\right|+\left|2Bd^4\right|+\left|2bd\right|\right)+\ln\left(\max\left|A\right|,\left|B\right|,1\right)$.
2. Existe uma constante C_E (dependendo só de E) tal que, para todo $P\in E$ $h\left(2P\right)\ge 4h\left(P\right)-C_E$, onde se pode tomar $C_E=\ln^2\left(\max k_i\right),\quad i=1,2,3,4$, com

$$k_1=12+16\left|A\right|;$$

$$k_2=3+\left|5A\right|+27\left|B\right|;$$

$$k_3=4\left|4A^3+27B^2\right|+4A^2\left|B\right|+4\left|A\left(3A^3+22B^2\right)\right|+12\left|B\left(A^3+8B^2\right)\right|;$$

$$k_4 = A^2|B| + \left|A\left(5A^3 + 32B^2\right)\right| + 2\left|B\left(13A^3 + 96B^2\right)\right| + 3\left|A^2\left(A^3 + 8B^2\right)\right|.$$

3. Se os pontos do conjunto $\{Q_1, Q_2, ..., Q_r\}$ são de representantes de $E(\square)/2E(\square)$ e $C' = \max\{C_{Q_i}\}$, com $i = 1, ..., r$. Então o conjunto $\{Q_1, Q_2, ..., Q_r\} \cup \left\{P \in E : h(P) \le 1 + \frac{C_E + C'}{2}\right\}$ é um sistema de geradores de $E(\square)$.

Proposição 2.5.3: Seja E uma curva elíptica e $k \in \square$. Então só há um número finito de pontos de $E(\square)$ com altura menor que k.

Demonstração

Dado que $h(x:y:z) = \ln\left(\max\{|x|, |z|\}\right)$ é óbvio que só uma quantidade finita de x e z podem verificar que $h(x:y:z) > k$. Pelo que se impusermos estes x e z achamos, para cada par, uma quantidade finita de y. Em consequência, a quantidade total de pontos em $E(\square)$ há-de ser finita.

Quase- algoritmo de cálculo de um sistema de geradores

Dados a e b, coeficientes na forma de Weierstrass:

1. Aplicamos o quase-algoritmo de cálculo do rango, com o qual achamos, em particular, $E(\square)/2E(\square)$;
2. Aplicamos a primeira proposição para achar a constante;
3. Calculamos os pontos com altura menor que uma constante fixa. Isto pode fazer-se algorítmicamente seguindo (mais ou menos) a demonstração da segunda proposição;
4. Os pontos achados nos passos 1 e 3 formam um sistema de geradores.

2.6 - Teorema de Mordell-Weil

Consideremos uma curva elíptica da forma:

$$E: y^2 = x^3 + ax + b = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$

Teorema (Mordell) 2.6.1: Seja E uma curva elíptica. Então existe um conjunto de pontos racionais $P_1, P_2, \ldots, P_n$ tal que, qualquer ponto racional da curva E se representa na forma: $P = a_1P_1 + a_2P_2 + \ldots + a_nP_n + Q$, onde $a_1, a_2, \ldots, a_n$ são números inteiros, univocamente definidos pelo ponto P e Q é um ponto racional de torção.

Por outras palavras, todos os pontos racionais numa curva elíptica, se obtêm do número finito desses pontos por meio de construção de secantes e tangentes.

Consideremos os exemplos A – D do ponto de vista de torção e rango.

A. A curva $y^2 = x^3 - 9x + 81$ não tem torção, isto é, o ponto O é o único ponto racional de torção nessa curva. O seu rango é igual a 2. Na qualidade dos pontos P_1, P_2 do teorema Mordell pode tomar os pontos $(-3,9)$ e $(0,9)$.

B. A curva $y^2 = x^3 - 36x$ tem quatro pontos racionais de torção: o ponto O e mais três do segundo grau. Seu rango é igual a 1, e na qualidade de P_1 pode tomar o ponto $(-2,8)$.

C. A curva $y^2 = x^3 - x + \frac{1}{4}$ não tem torção. O seu rango é igual a 1, na qualidade do ponto P_1 pode tomar o ponto $\left(0, \frac{1}{2}\right)$.

D. A curva de Fermat $y^2 = x^3 - \frac{1}{108}$ tem três pontos racionais de torção: O e dois pontos de grau três. O seu rango é igual a 0.

Seja $E: y^2 = x^3 + ax + b = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$

Teorema 2.6.2: O conjunto $E(\square) \subset E$ de pontos racionais de uma curva E é subgrupo do grupo E.

Este é o grupo em que nós centraremos a nossa atenção. O resultado mais importante que este grupo concerne foi conjecturado por Poincaré em 1901 e demonstrado por L.J. Mordell em 1922. Nos anos 40 foi generalizado por Weil para corpos de números algébricos e dai o nome – Teorema Mordell-Weil.

Teorema (Mordell-Weil) 2.6.3 O grupo $E(\square)$ está finitamente gerado.

Como é habitual, há duas versões diferentes da demonstração: uma algébrica e abstracta e outra mais orientada para o cálculo explícito dos geradores de grupo.

Em qualquer caso, todas as demonstrações se dividem em duas partes: o m-descenso (o teorema débil de mordell-Weil) e o descenso infinito.

A primeira parte consiste em provar que o grupo quociente $E(\square)/mE(\square)$ é finito.

A segunda consiste em utilizar este resultado para provar que o grupo $E(\square)$ é finitamente gerado.

Teorema (Débil de Mordell-Weil) 2.6.4: O $E(\square)/2E(\square)$ é um grupo finito.

A demonstração deste teorema, requer quatro lemas técnicos. Enunciaremos sem demonstração e fazemos alguns comentários.

Lema 2.6.1: Sejam $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ pontos da curva E. Sejam $Q = (x_3, y_3)$ o ponto de intersecção de P_1P_2 com E e $R = (x_4, y_4)$ outro ponto de intersecção de E com a sua tangente em P_1. Então:

$$x_3 = \frac{(x_1x_2 + a)(x_1 + x_2) + 2b - 2y_1y_2}{(x_1 - x_2)^2}$$

$$x_3 - \alpha_i = \frac{\left[y_1(x_2 - \alpha_i) - y_2(x_1 - \alpha_i)\right]^2}{(x_1 - \alpha_i)(x_2 - \alpha_i)(x_1 - x_2)^2}$$

$$x_4 = \frac{x_1^4 + a^2 - 8bx_1 - 2\alpha x_1^2}{4(x_1^3 - ax_1 + b)}$$

$$x_4 - \alpha_i = \left(\frac{x_1^2 + a - 2\alpha_i x_1 - 2\alpha_i^2}{2y_1} \right)^2$$

Lema 2.6.2: Consideremos os três pontos $P_i = (\alpha_i, 0)$ e seja $P = (x, y) \in E$, com $y \neq 0$. Nestas condições a primeira coordenada de $P + P_i$, x_0 verifica que $x_0 - \alpha_i = (x - \alpha_i)(x - \alpha_j)(x - \alpha_k) S^2$, para algum $S \in \mathbb{Q} \setminus \{0\} = \mathbb{Q}^*$.

Sejam, para $i = 1, 2, 3$ as aplicações

$$\phi_i : E(\mathbb{Q}) \to \mathbb{Q}^* / \mathbb{Q}^{*2}$$

$$O \mapsto 1.\mathbb{Q}^{*2}$$

$$(x, y) \mapsto (x - \alpha_i).\mathbb{Q}^{*2}$$

$$(\alpha_i, 0) \mapsto (\alpha_i - \alpha_j)(\alpha_i - \alpha_k).\mathbb{Q}^{*2}$$

Lema 2.6.3: As aplicações ϕ_i, são homomorfismos de grupos, para $i = 1, 2, 3$.

Este lema demonstra-se de forma quase imediata utilizando os dois lemas anteriores, assim como feito de que $P_i + P_j = P_k$.

Lema 2.6.4: $\bigcap_{i=1}^{3} \ker(\phi_i) \subset 2E(\mathbb{Q})$

Este lema demonstra-se directamente, tomando um ponto P na intersecção dos núcleos e encontrando um ponto Q tal que $P = 2Q$.

O teorema de débil de Mordell-Weil pode ser provado agora, da seguinte maneira.

Demonstração

Partindo do último lema, basta demonstrar que o grupo quociente $E(\mathbb{Q}) / \left(\bigcap \ker(\phi_i) \right) \supset E(\mathbb{Q}) / 2E(\mathbb{Q})$ é finito. Isto é, que as imagens da aplicação ϕ_i são finitas. Para tal, tomamos um ponto $(x, y) \in E(\mathbb{Q})$ e escrevemos na forma

$$x = \frac{r}{t^2};\ y = \frac{s}{t^3};\ (r, t^2) = (s, t^3) = 1, \text{ como } (x, y) \in E$$

tem-se que

$\left(r-\alpha_1 t^2\right)\left(r-\alpha_2 t^2\right)\left(r-\alpha_3 t^2\right)=s^2$ de forma que a imagem por ϕ_i de (x,y) há-de ser

$$\phi_i(P)=(x-\alpha_i).\square^{*2}=u.\square^{*2}$$

Donde se pode demonstrar que há um número finito de possibilidades para u.

Para a parte do descenso infinito necessitamos de um novo conceito: a <u>altura de um ponto</u>.

Definição 2.6.1: A altura de um ponto $(x:y:z)\in E$, com $x,y,z\in\square$ e $(x,y,z)=1$ é

$$h(P)=\ln\left(\max\left\{|x|,|z|\right\}\right)$$

Vejamos algumas propriedades (lemas) da altura:

Lema 2.6.5: Seja $P=(x:y:z)$ um ponto da curva E, então:

1) $\ln\left(y^2z\right)\le 3h(P)+C_1$, com C_1 dependendo só de E
2) Há uma constante C_P, que depende de P, tal que, para todo $Q\in E$,
$$h(P+Q)\le 2h(P)+C_P$$
3) Dada uma constante $k\in\square$, existe um número finito de pontos da curva com altura menor que k.

OBS: Estas propriedades são imediatas, nos casos 1) e 3), e directa do primeiro lema do teorema débil de Mordell-Weil no caso 2).

Lema 2.6.6: Há uma constante C_3 que depende de E tal que, para todo $P\in E$,

$$3h(P)\le h(2P)-C_3$$

Podemos agora demonstrar o teorema de Mordell-Weil.

<u>Demonstração</u>

Suponhamos que temos:

$E(\square)/2E(\square)=\{Q_1,...,Q_r\}$, e tomemos um ponto $P=P_0$.

Definimos o ponto P_{n+1} de maneira recorrente, como

$$P_n = Q_i + 2P_{n+1}, \text{ para algum } Q_i .$$

Dos lemas prévios temos que

$$-C_3 + 3h(P_{n+1}) \le 2h(P_n) + C_4, \text{ onde } C_4 = \max\ C_{Q_i}\ \ (i = 1,...,r).$$

Então para algum constante C

$$h(P_{n+1}) \le \frac{C}{3} + \frac{2}{3}h(P_n), \text{ onde voltando atrás temos}$$

$$h(P_{n+1}) \le C\left(\frac{1}{3} + \frac{1}{3^2} + ... + \frac{1}{3^n}\right) + \left(\frac{2}{3}\right)^n h(P_0).$$

Tomando limite, encontramos que P pode ser construído a partir dos Q_i, mas todos os pontos de altura menor que certa constante, independente de P, que também são em quantidade finita.

OBS: Os algoritmos para calcular a torção, o rango e geradores de grupo não são fáceis de calcular. Por isso, para facilitar o cálculo de exemplos concretos, apresentamos em anexo alguns programas de MAPLE para os calular.

CONCLUSÃO

Com a realização deste trabalho foram atingidos os objectivos propostos, salientando o facto de ter ficado com um horizonte muito alargado em relação ao tema em questão.

De facto, pude constatar que as "**Curvas Elípticas**" é um tema muito interessante para as investigações futuras e podemos considerá-las como uma fonte muito rica em informações que faz conexões com a maioria ou se não com todas as áreas da Matemática.

Do ponto de vista teórico-metodológico, foi possível efectuar um estudo cuidadoso do comportamento das curvas elípticas abordando as definições e as propriedades a ela inerentes, fazendo algumas ilustrações para uma melhor compreensão das mesmas.

Eventualmente que, o desenvolvimento na íntegra deste tema é algo que requer um tratamento muito mais aprofundado do que foi dado neste trabalho, o que implicaria o envolvimento de maiores recursos bibliográficos e, sobretudo um domínio de conhecimentos que ainda precisam ser adiquiridos.

Naturalmente que, uma pessoa ao ver o tema do nosso trabalho e mesmo depois de o ler pode levantar a seguinte questão: "***Será que existe alguma ligação entre o tema do nosso trabalho e uma elipse***?". Podemos deixar uma pequena pista, uma vez que não consta no objectivo do nosso trabalho, que é a seguinte: uma curva elíptica não é uma elipse! A razão para o nome é um pouco mais indirecta. Tem uma ligação com o cálculo do comprimento de arco de uma elipse. Este facto pode ser um ponto de partida para uma nova pesquisa.

No entanto, num futuro próximo pode-se dar continuidade a este trabalho.

BIBLIOGRAFIA

- CASTILLO, Carlos Ivorra : “Curvas Elípticas”
- MILNE, J. S. : “Elliptic Curves”, August 21, 1996; v1.01.
- Ostrik V. V., Tcfasman M. A., “Geometria algébrica e teoria dos números: curvas racionais e elípticas”. Moscovo, 2001. Biblioteca da educação Matemática.
- TORNERO, José M. : “Puntos Racionales em Curvas Elípticas”, Septiembre, 1996.

Sites da Internet

http://mathworld.wolfram.com/contact/

http://cgd.best.vwh.net/home/flt/fltmain.htm

http://mathwolfram.com/weiesrtrassEllipticFunction.html

http://mathwolfram.com/RationalPoint.html

ANEXOS

PROGRAMAS DE MAPLE

Os programas que vamos apresentar aqui, são programas para facilitar o cálculo de exemplos concretos.

OBS: As constantes A e B que estão a ser utilizados nestes programas e as que nós utilizamos na forma breve de Weierstrass – $y^2 = x^3 + ax + b$ são iguais.

1. swform – calcula o discriminante da forma breve de Weierstrass;

```
swform:= proc(l:list)
   local b2,b4,b6,b8,c4,c6,i,r,ratsols,sols,A,B,D,DISC,EQN;
   if nops(l)<>5 then
      ERROR(`Enter a list with the form [a1,a2,a3,a4,a6]`);
   fi:
   b2:= l[1]^2+4*l[2];
   b4:= 2*l[4]+l[1]*l[3];
   b6:= l[3]^2+4*l[5];
   b8:= l[1]^2*l[5]+4*l[2]*l[5]-l[1]*l[3]*l[4]+l[2]*l[3]^2-l[4]^2;
   c4:= b2^2-24*b4;
   c6:= -b2^3+36*b2*b4-216*b6;
   DISC:= -(b2)^2*b8-8*b4^3-27*b6^2+9*b2*b4*b6;
   A:= -c4*27;
   B:= -c6*54;
   EQN:= Y^2 = X^3+A*X+B;
   print(`Discriminant:`);
   print(ifactor(DISC));
   print(`Short Weierstrass form:`);
   print(EQN);
   print(`Discriminant of the short Weierstrass form:`);
   print(ifactor(4*A**3-27*B**2));
   sols:= map(simplify,[(solve(subs(Y=0,EQN),X))]);
   ratsols:= []:
   for i from 1 to 3 do
       if type(sols[i],rational) then
          ratsols:= [op(ratsols),sols[i]];
       else
          ratsols:= ratsols:
       fi:
```

```
    od:
    print(`Rational points of torsion two are:`);
    if nops(ratsols)=0 then
       RETURN(`None.`);
    else
       for i from 1 to nops(ratsols) do
           r[i]:= [ratsols[i],0];
           print(r[i]);
       od;
    fi:
end:
```

2. reduction – calcula o número de pontos que há em $E(\mathrm{F}_P)$;

```
reduction:= proc(l:list,p:integer)
   local A,B,i,j,k:
   A:= irem(l[1],p):
   B:= irem(l[2],p):
   k:= 0:
   for i from 0 to p-1 do
       for j from 0 to p-1 do
           if irem(i^2 - j^3 - A*j - B,p) = 0 then
              k:= k+1:
           else
              k:= k:
           fi:
       od:
   od:
   print(`The number of points of the reduced curve is:`);
   RETURN(k+1);
end:
```

3. torpoints – calcula seguindo o teorema de Nagell-Lutz, um conjunto onde estão todos os possíveis e mais alguns pontos de torção;

```
torpoints:= proc(l:list)
   local A,B,EQN,d,div,divisors,exp,i,j,k,newdiv,points,sols:

   with(numtheory):
   A:= l[1]:
   B:= l[2]:
   EQN:= Y^2 = X^3+A*X+B;
   d:= ifactors(4*A^3 + 27*B^2):
   d:= d[2]:
   div:= []:
   for i from 1 to nops(d) do
       if d[i][2]>1 then
          div:= [op(div),d[i]]:
       fi:
   od:
   divisors:= [0,1]:
   for i from 1 to nops(div) do
       exp:= iquo(div[i][2],2):
       newdiv:= []:
       for j from 0 to exp do
           for k from 1 to nops(divisors) do
               newdiv:= [op(newdiv),divisors[k]*(div[i][1]^j)]:
           od:
       od:
       divisors:= [op(divisors),op(newdiv)]:
   od:
   divisors:= convert(divisors,set):
   divisors:= convert(divisors,list):
   points:= {}:
   for i from 1 to nops(divisors) do
       sols:= [solve(subs(Y=divisors[i],EQN),X)]:
       for j from 1 to nops(sols) do
           if type(sols[j],integer) then
              points:= {op(points),[sols[j],divisors[i]]}
           fi:
       od:
   od:
   print(`The only possible non-zero torsion points are:`);
   print(points);
   print(`and their reflections in the X-axis.`);
end:
```

4. torsion – calcula os pontos de torção;

```
torsion:= proc(l:list)
   local A,B,Disc,P,div,h,i,j,k,n,m,prime,r,ratsols,sols,t:
   A:= l[1]:
   B:= l[2]:
   Disc:= 4*A**3-27*B**2:
   prime:= 11:
   n:= (12!)/11:
   while prime<31 do
         if irem(Disc,prime)=0 then
            prime:= nextprime(prime):
         else
            m:= reduction(l,prime):
            n:= igcd(n,m):
            prime:= nextprime(prime):
         fi:
   od:
   sols:= [solve(X**3+A*X+B,X)]:
   ratsols:= []:
   for i from 1 to 3 do
       if type(sols[i],rational) then
          ratsols:= [op(ratsols),sols[i]];
       else
          ratsols:= ratsols:
       fi:
   od:
   if nops(ratsols)=n-1 then
      print(`The torsion points are those of order two:`)
      for i from 1 to nops(ratsols) do
          r[i]:= [ratsols[i],0];
          print(r[i]);
      od:
      RETURN(`and O = [0,1,0]`);
   fi:
   t:= torpoints(l):
   div:= convert(divisors(n),list):
   for i from 1 to nops(t) do
       P:= t[i]:
       for j in div do
           for h from 1 to j do
               P:= chtang(l,[t[i],P]):
           od:
           if P=[0,1,0] then
              print(`Punto:`,t[i]):
              print(`Orden:`,j):
```

```
            elif P[2]=0 then
               print(`Punto:`,t[i]):
               print(`Orden:`,2*j):
            fi:
         od:
    od:
end:
```

Os programas 6 e 7 calculam as constantes intermédias necessárias para o descenso infinito.

5. pconst – calcula a constante que depende do ponto;

```
pconst:=proc(l:list, p:list)
   local A,B,C,C_1,C_2,a,b,d,x,y:
   A:= l[1]:
   B:= l[2]:
   x:= p[1]:
   y:= p[2]:
   d:= lcm(denom(x),denom(y)):
   a:= numer(x)*(d^2/denom(x)):

   b:= numer(y)*(d^3/denom(y)):
   C_1:= abs(a*d^2) + abs(A*d^4) + abs(A*d^2*a) +
         abs(2*B*d^4) + abs(2*d*b):
   C_2:= max(abs(A), abs(B), 1):
   C:= evalf(ln(C_1*C_2)):
   RETURN(C);
end:
```

6. cconst – calcula a constante que depende só da curva;

```
cconst:=proc(l:list)
   local A,B,C_E,C_0,k_1,k_2,k_3,k_4:
   A:= l[1]:
   B:= l[2]:
   k_1:= 12 + 16*abs(A):
   k_2:= 3 + abs(5*A) + abs(27*B):
   k_3:= 4*abs(4*A^3+27*B^2) + 4*abs(A^2*B) +
```

```
        + 4*abs(A*(3*A^3+22*B^2)) + 12*abs(B*(A^3+8*B^2)):
  k_4:= abs(A^2*B) + abs(A*(5*A^3+32*B^2)) +
        + 2*abs(B*(13*A^3+96*B^2)) + 3*abs(A^2*(A^3+8*B^2)):
  C_0:= max(k_1,k_2,k_3,k_4):
  C_E:= evalf((ln(C_0))^2):
  RETURN(C_E);
end:
```

7. **bound** – calcula os pontos da curva com altura menor que um número real fixo;

```
bound:=proc(l:list,n:numeric)
   local A,B,i,j,k,points,x,y:
   A:= l[1]:
   B:= l[2]:
   points:= {}:
   k:= 1:
   while k<evalf(exp(n)) do
      k:= k+1:
   od:
   if type(sqrt(B),rational) then
      points:= {op(points), [0,sqrt(B)], [0,-sqrt(B)]}:
   fi:
   for i from 1 to k do
       for j from 1 to i*k do
           if gcd(i,j)=1 then
              x:= j/i:
              y:= sqrt(x^3+A*x+B):
              if type(y,rational) then
                 points:= {op(points), [x,y], [x,-y]}:
              fi:
           fi:
       od:
   od:
   print(`The points are:`);
   RETURN(points);
end:
```

8. infdesc – calcula, usando as rotinas anteriores, um conjunto de geradores de $E(\square)/2E(\square)$;

```
infdesc:=proc(l:list,s:list)
   local A,B,C,C_0,C_E,const,i:
   A:= l[1]:
   B:= l[2]:
   C_E:= cconst(l):
   const:= []:
   for i from 1 to nops(s) do
       const:= [op(const), pconst(l,s[i])]:
   od:
   C_0:= max(op(const)):
   C:= 2 + (C_E + C_0)/2:
   bound(l,C);
end:
```

9. sieve – calcula um sistema de geradores minimal.

```
sieve=proc(w:list,l:list,n:integer)
   local coeff,i,j,l,n,m,p,prov,x,w:
   x:= {}:
   for i from 1 to nops(l) do
       x:= {op(x),l[i][1]}:
   od:
   p:= l:
   m:= convert(p,set):
   coeff:= 1:
   while nops(m)>n do
         coeff:= coeff+1:
         for j from 1 to nops(p) do
             prov:= p[j]:
             for i from 2 to coeff do
                 prov:= chtang(w,[p[j],prov]):
```

```
                od:
                if member(prov[1],x) then
                   p:= p minus [p[j]]:
                   m:= convert(p,set):
                fi:
            od:
    od:
    print(`The independent generators are:`):
    RETURN(m);
end:
```